Los Angeles County Registrar-Recorder/County Clerk

DEAN C. LOGAN
Registrar-Recorder/County Clerk

Testimony to Joint Informational Hearing
"Cybersecurity and California Elections"
Assembly Committee of Elections and Redistricting and
Senate Committee on Elections and Constitutional Amendments

March 7, 2018

Dean C. Logan
Los Angeles County Registrar-Recorder/County Clerk

Good morning Chairman Berman, Chairman Stern and members of the Committees. I am Dean Logan, the Registrar-Recorder/County Clerk for the County of Los Angeles. I am here today both in my capacity as the chief elections official for Los Angeles County and on behalf of the California Association of Clerks and Election Officials. Thank you for the opportunity to be part of today's conversation on Cybersecurity and California Elections.

First and foremost, on behalf of the 58 County Registrars of Voters who represent the boots on the ground of election administration in the State, I want to convey how seriously we take the security and integrity of the elections process. Local and state election officials in California are actively engaged on system security and exercising diligence in monitoring for threats and vulnerabilities that undermine our elections process.

As you have heard, we have been given no specific information to demonstrate that any of California election systems were compromised and the intelligence community has repeatedly confirmed that the tabulation of votes in the 2016 election was not manipulated or altered; however without question our awareness and alertness is heightened based on the recognizable activity and threats that have been referenced in your briefing packets and by previous speakers.

What is clear is that there are bad actors actively trying to disrupt the elections process and that threat is compounded by inconsistent information sharing and incident reporting. As we move into another major election cycle, it is incumbent on all of us – federal, state and local officials – to be vigilant about security while encouraging active voter participation to demonstrate the strengths of our representative-based form of government.

With respect to cybersecurity preparedness for elections, there are two important points to remember:

First, cybersecurity is no different for elections than it is for other critical sectors including healthcare, public safety or financial services. The best cybersecurity practices adopted by Information Technology (IT) professionals across the spectrum of government and industry are equally applicable to elections administration and strict adherence to those practices is essential to election security.

Second, cybersecurity involves several layers of protection against attacks, including physical security, general IT security protocols and system-specific security features. Each of these layers is present in the cybersecurity defenses protecting elections infrastructure at the county level – and each involves people and processes in addition to hardware, software and facilities.

We remain confident that our systems – despite their age and limited agility – in combination with the appropriate safeguards and protocols, can ensure a secure election environment in 2018. That said, it remains incumbent upon us to be vigilant in monitoring our systems activity and adhering to operational protocols that are essential to IT security and election transparency.

It is important to note that much of the concern raised about interference in the elections process (in the United States and abroad) is related to activity outside the scope of voting systems and election administration. Significant concerns and allegations have centered around interference with political data sources and with false or misleading social media messaging using bots, etc. This activity has been validated and documented by multiple sources and remains a consistent theme in national media coverage of the 2016 election and projection of activity in the 2018 cycle.

While we do not have direct ability to combat or regulate the activity external to the voting systems and processes, we do see this as an integral element of voter outreach and education. In that regard, we will seek to establish and promote trusted sources for voters who seek information about the voting process – when, where and how to cast a ballot, etc. We will also actively share any clarifications or warnings that can help voters identify information that is not coming from trusted sources. Maintaining the resources for notification systems and for broad outreach and education activity is critical to this effort.

In addition to what has already been covered in today's hearing, it is also important to acknowledge that the security threats and vulnerabilities referenced link to a resource issue. While California benefits from a policy foundation that helps ensure security including a well-established voting system certification process; the requirement for paper-based ballots that can be verified by voters and that are subject to post-election auditing; a clear emphasis on transparency and accountability; and a set of voting systems standards that support future development and innovation; the reality is that our core elections infrastructure is largely outdated and unmatched to that policy foundation.

Most counties in the State are relying on technology and equipment for voting that is more than ten-to-fifteen years old and reliant on user interfaces that lack the accessibility and functional capabilities to meet the needs and expectations of a large, diverse and complex electorate. We also lack a stable source of funding to invest in modernized solutions to address those challenges.

In Los Angeles County, our core voting system components date back to 1968 when punch card voting was first introduced in California – a date that pre-dates the birth of the previous speakers, your two committee chairs and the vast majority of the team we have assembled to identify and implement the new voting experience in Los Angeles County. Efforts and plans to modernize have been stymied by a shrinking and insufficient proprietary market and, at times, an unstable and inflexible regulatory structure.

We are now on the cusp of introducing our "Voting Solutions for All People" initiative aligned to the voting model envisioned in the Voter's Choice Act and grounded in publicly-owned, open source developed voting interfaces and system components. Security is a high priority for us, it is one of our core principles. The voting system will have features for safe and secure storage

including robust chain of custody protocols and features such as locks and security seals to protect the integrity of the equipment while in the custody of election workers or in storage with election officials. In pursuing this effort, we established and worked closely with a Technical Advisory Committee that included highly-respected and nationally recognized experts in security. And, we will engage in third-party testing and hacking exercises prior to deployment.

Scheduled to be fully implemented in the 2020 election cycle, the new model is designed to be secure and transparent for all voters. There are various system elements that protect the integrity of elections and the voting process. Those elements are outlined in the background materials provided in your briefing packets and represent a framework for security that should be aligned to future development and procurement of voting systems in California.

Fully realizing the benefits and security provisions of the new Los Angeles County model and others like it will require a funding commitment to support the initial investment, necessary outreach and education, and implementation. The Governor has included $134 million in voting system modernization funding in his proposed budget. This signals a recognition of the need and a commitment of support, but it falls short of what is needed. Your support is needed to increase and continue the funding in future budgets until we have replaced and implemented new voting systems throughout California consistent with this discussion on security.

In closing, I want to assure you that my colleagues and I are actively engaged on the State and national levels in ongoing discussions, information sharing and collaboration around cybersecurity and election integrity. As new information is disseminated from the intelligence community, we ensure all counties are well informed. As recommendations regarding security protocols, checklists and tools are made available, we move swiftly to ensure our processes and procedures are aligned.

We recognize the significance this dialogue and our response has on voter confidence and participation. We appreciate your commitment to raising the profile of these issues in California and we stand ready to work in partnership with the U.S. Election Assistance Commission, the Department of Homeland Security, the Secretary of State and the Legislature in the administration of the 2018 state elections.

Thank you.